

TCP/IP İle İşletim Sistemi Saptama

İşletim sistemi saptamak karmaşık işlemlerden oluşan bir süreçtir. İşletim sistemlerinin (Windows, Linux, FreeBSD, Solaris vs.) ağ üzerinden aldıkları paketlere verdikleri tepkiler bazı durumlarda farklılıklar göstermektedir, bu farklılıkların doğru analiz edilmesi, hedef işletim sistemini ele verecek ipuçlarını da ortaya çıkarır. Bu farklılıkları analiz eden ve işletim sistemine göre farklılıkların kaydedildiği bir veritabanı ile karşılaştırarak yorumlayan bazı programlarda geliştirilmiştir.

İşletim sistemi saptama süreci, ağ haritalama ve ağa sızma testlerinin önemli parçalarındandır. Düzenlenecek saldırı ve zayıflık denetimlerinin hedefe özel olması gerekliliği bu tekniğin gelişmesine sebep olmuştur. Birçok saldırgan, hedef sistemde bulunan zayıflıkları incelemek için özel programlar kullanmak yerine, hedef hakkında bilgi toplamayı ve böylece zayıflıkları bulmayı tercih eder; bu durumda faydalandığı önemli tekniklerden biride hedefin işletim sisteminin ve uygulamalarının saptanmasıdır.

İşletim sistemi saptama teknikleri zaman içerisinde değişiklikler yaşamış, geliştirilmiş ve üst seviye bilgiye gereksinim duyulmayan araçlar ile otomatize edilmiştir. Genel olarak 2 yöntem ile işletim sistemi saptanır ; Aktif denetim ve Pasif denetim.

Aktif denetim , Queso aracı ile duyulmaya başlamıştır. Temel fikir hedefe özel paketlerin gönderilmesi ve alınan cevapların bir veritabanı ile karşılaştırılmasıdır. Queso bu tekniği başarı ile uygulayan ilk araçtır. Hedef sisteme çeşitli TCP paketleri göndererek aldığı paketlerin analizini yapmaktadır. Ancak bu tekniği uygulayan ilk araç olmasının getirdiği eksiklikler Fyodor tarafından görülmüş ve Queso'nun kullandığı teknikler geliştirilerek Nmap isimli araca eklenmiştir. Queso'nun geliştirilmesi bir süre sonra durduruldu ; ancak Nmap aracı halen gelişimine devam etmektedir, sadece bir işletim sistemi saptama aracı olmaktan çok daha fazla özelliğide bünyesinde barındırmaktadır. Fyodor, Nmap'in işletim sistemi saptamada kullandığı teknikleri ayrıntılarıyla açıklayan bir dökümanında hazırlamış ve sitesinde yayınlamaktadır. Hedefe FIN bayraklı TCP paketi göndermek, IP paketlerinin çerçeve boyunda değişiklikler yapmak ve TCP paketindeki normalde beraber aktif olmayan bayrakları aynı anda aktif ederek hedefe göndermek, bu tekniklere birkaç örnektir.

Ofir Arkin'in yazmış olduğu "ICMP Usage in Scanning" isimli dökümanda açıklanan yöntem, aktif işletim sistemi saptama yöntemlerine bir yenisini eklemiştir. Temel fikir, hedefe çeşitli ICMP paketleri (Echo Request, TimeStamp Request vs.) , bozuk IP paketleri ve UDP paketleri göndermek ve alınan cevapları bir karar ağacı doğrultusunda değerlendirmektir. Örneğin; ağ yayın adresine gönderilen "ICMP/Echo Request" paketine Windows türevi işletim sistemleri cevap vermemektedir, böylece bu pakete cevap gönderen sistemlerin Windows türevi bir işletim sistemi olmadığı anlaşılmış olur. Dökümanın üçüncü sürümünden sonra, Ofir Arkin ve Fyodor Yarochkin tarafından hazırlanan Xprobe isimli araçta, dökümanda açıklanan teknikleri uygulamaktadır.

Aktif denetim yönteminde, gönderilecek paketlerin özel olabilmesi ve denetimin daha fazla türde paket üzerinden yapılması, yanlış payını düşürmektedir ; ancak bu tür denetimlerin saldırı tespit sistemleri tarafından kolayca farkedilebilir olması, katlanılması gereken ciddi bir risktir. Bu riskin oluşmaması ve elde edilen sıradan paketler ile de işletim sistemi saptayabilmek için Pasif denetim yöntemi geliştirilmiştir. Pasif denetim yönteminde, hedefin bu tür bir denetimi farketmesi mümkün değildir ; ancak denetimde özel paket gönderilmemesi ve alınacak paket türlerinin kısıtlı olması yüksek yanlış oranında beraberinde getirmektedir.

Pasif denetim yönteminde, hedefe sıradan ve izin verilen bağlantılar kurulur (Örn. Web sayfası gezmek ve FTP ile dosya aktarımı yapmak) ve hedeften alınan paketler analiz edilir. Paketlerin içerdiği; TOS (Type of Service), TTL ve paket bölünme şekli gibi bilgiler ile işletim sistemlerinin saptanması mümkün olmaktadır. Çoğu işletim sisteminin TCP/IP yığınının farklı olması bu tekniğin geliştirilmesine yardımcı olmuştur. Bu yöntemi uygulamak için geliştirilmiş bazı araçlarda mevcuttur ; Siphon, POf ve Passfing bu araçların başarılı olanları arasındadır. Bu araçlar bir sniffer gibi çalışarak gelen paketleri analiz edebileceği gibi daha önceden Tcpdump ile yakalanmış paketleride analiz edebilmektedir.

TCP/IP paketlerinin analizi ile işletim sistemini saptayan bu yöntemlere ek olarak servis açılış mesajları, bağlanılan servislerdeki bilgi istekleri ve hata mesajlarında, hedef işletim sistemi hakkında çeşitli bilgileri barındırmaktadır. Bu tür bilgilerin harmanlanması ile bulunacak sonucun yanılma payıda düşük olacaktır.

Hedefin işletim sisteminin ve yama seviyesinin belirlenmesi, hedefe özel güvenlik denetimlerinin önemli parçalarından biridir. Saldırı tespiti, ağ haritalama ve ağa sızma testleri gibi süreçlerde bu yöntemlere sıkça başvurulmaktadır.

Fatih Özavcı

Security Analyst

holden@siyahsapka.com

<http://www.siyahsapka.com>

<http://www.dikey8.com>

Ek 1 – Araçlar

Queso

Nmap <http://www.insecure.org/nmap>

Xprobe <http://www.sys-security.com/html/projects/X.html>

Siphon <http://siphon.datanerds.net>

POf <http://lcamtuf.coredump.cx>

Passfing

Ek 2 – Makaleler

Fyodor – Remote OS detection via TCP/IP Stack FingerPrinting

<http://www.insecure.org/nmap/nmap-fingerprinting-article.html>

Ofir Arkin – ICMP Usage In Scanning

http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf

Ofir Arkin / Fyodor Yarochkin – X Remote ICMP Based OS Fingerprinting Techniques

http://www.sys-security.com/archive/papers/X_v1.0.pdf

Honeynet Project – Know Your Enemy : Passive Fingerprinting

<http://project.honeynet.org/papers/finger>